Amendments to the Claims:

Claims 1-28 are pending in this application. Please amend claims 1, 11, 13, 16, 20, and 24 as follows:

1. (currently amended) A system for multi-stream security processing and distributing digital media streams, the system comprising:

a headend configured to generate encrypted digital media streams and download software;

a network coupled to the headend and configured to receive the encrypted digital media streams and downloaded software; and

at least one receiver coupled to the network and configured to receive the encrypted digital media streams and downloaded software and to present a decrypted version of the encrypted digital media streams based on the downloaded software, wherein ~~at least one of the headend and~~ the ~~at least one~~ receiver comprises a security processor configured to provide at least one of simultaneous multiple encryption and simultaneous multiple decryption processing of the digital media streams, the security processor operative to store the downloaded software and to securely configure, renew, and re-configure at least one of encryption and decryption by the security processor based on the downloaded software.

2. (original) The system of claim 1 wherein the media streams are at least one of a video stream, and audio stream, and a video plus audio stream.

3. (original) The system of claim 1 wherein the security processor comprises a plurality of digital stream encryption/decryption engines that are selectively parallel coupled by a controller for simultaneous operation in response to a predetermined security configuration.

4. (original) The system of claim 3 wherein the security configuration comprises at least one of Data Encryption Standard (DES), Triple DES (3-DES), Advanced Encryption Standard (AES), and Common Scrambling Algorithm (CSA).

5. (original) The system of claim 3 wherein the security configuration comprises at least one of a secure download, RSA key management, multiple security key management, authentication, copy protection, and digital signatures.

6. (original) The system of claim 3 wherein the security processor further comprises at least one of a memory containing a hash, engine encryption/decryption configuration logic, a random number generator, a multiplier, and a memory containing a dynamic feedback arrangement scrambling technique (DFAST) algorithm coupled in parallel to the controller and configured to provide multiple key management for at least one of conditional access and digital rights management.

7. (original) The system of claim 3 wherein the security processor further comprises at least one of a swappable random access memory (RAM) and a swappable flash memory containing the predetermined security configuration.

8. (original) The system of claim 3 wherein the security processor provides role-based authentication that is used by an authorized user for at least one of configuration, reconfiguration, and renewal.

9. (original) The system of claim 1, wherein the receiver is at least one of a set top box (STB), and a receiver or transceiver for at least one of digital televison, high definition digital television (HDTV), audio, MP3, text messaging, and game digital streams.

10. (original) The system of claim 1, wherein the receiver is a set top box (STB) and the system further comprises an additional receiving device including the security processor, coupled to the STB and configured to receive and decrypt the encrypted digital media streams using the security processor.

11. (currently amended) A method of multi-stream security processing and distributing digital media streams, the method comprising:

generating encrypted digital media streams at a headend;

coupling a network to the headend and receiving the encrypted digital media streams at the network; ~~and~~

coupling a receiver ~~at least one receiver~~ to the network, the receiver receiving a software download from the network; ~~and~~

receiving the encrypted digital media streams at the receiver, and presenting a decrypted version of the encrypted digital media streams using the receiver~~, wherein at least one of the headend and the at least one receiver comprises~~;

re-configuring a security processor ~~configured~~ in the receiver based on the software download to provide at least one of simultaneous multiple encryption and simultaneous multiple decryption processing of the digital media streams; and

storing the software download in the security processor.

12. (original) The method of claim 11 wherein the media streams are at least one of a video stream, and audio stream, and a video plus audio stream.

13. (currently amended) The method of claim 11 wherein the security processor comprises a plurality of digital stream encryption/decryption engines that are selectively ~~parallel~~ coupled by a controller for simultaneous operation in response to a predetermined security configuration.

14. (original) The method of claim 13 wherein the security configuration comprises at least one of Data Encryption Standard (DES), Triple DES

(3-DES), Advanced Encryption Standard (AES), and Common Scrambling Algorithm (CSA).

15. (original) The method of claim 13 wherein the security configuration comprises at least one of a secure download, RSA key management, multiple security key management, authentication, copy protection, and digital signatures.

16. (currently amended) The method of claim 13 wherein the security processor further comprises at least one of a memory containing a hash, engine encryption/decryption configuration logic, a random number generator, a multiplier, and a memory containing a dynamic feedback arrangement scrambling technique (DFAST) algorithm coupled ~~in parallel~~ to the controller and configured to provide multiple key management for at least one of conditional access and digital rights management.

17. (original) The method of claim 13 wherein the security processor further comprises at least one of a swappable random access memory (RAM) and a swappable flash memory containing the predetermined security configuration.

18. (original) The method of claim 11 further comprising:

presenting the encrypted digital media streams from the receiver; and

coupling an additional receiving device including the security processor to the receiver and receiving and decrypting the encrypted digital media streams at the receiving device using the security processor.

19. (original) The method of claim 11 wherein the security processor provides role-based authentication that is used by an authorized user for at least one of configuration, reconfiguration, and renewal.

20. (currently amended) For use in a system for multi-stream security processing and distributing digital media streams, a security processor configured to provide at least one of simultaneous multiple media stream decryption and encryption processing, the security processor comprising:

a controller operative to be programmed through authenticated firmware downloads from a headend, each firmware download operative to modify media stream processing by the security processor;

a memory for storing the downloaded firmware; and

a plurality of digital stream encryption/decryption engines that are selectively ~~parallel~~ coupled by the controller for simultaneous operation in response to a predetermined security configuration downloaded to the controller.

21. (original) The security processor of claim 20 wherein the media streams are at least one of a video stream, and audio stream, and a video plus audio stream.

22. (original) The security processor of claim 20 wherein the security configuration comprises at least one of Data Encryption Standard (DES), Triple DES (3-DES), Advanced Encryption Standard (AES), and Common Scrambling Algorithm (CSA).

23. (original) The security processor of claim 20 wherein the security configuration comprises at least one of a secure download, RSA key management, multiple security key management, authentication, copy protection, and digital signatures.

24. (currently amended) The security processor of claim 20 wherein the security processor further comprises at least one of a memory containing a hash, engine encryption/decryption configuration logic, a random number generator, a multiplier, and a memory containing a dynamic feedback arrangement scrambling

technique (DFAST) algorithm coupled ~~in parallel~~ to the controller and configured to provide multiple key management for at least one of conditional access and digital rights management.

25. (original) The security processor of claim 20 wherein the security processor further comprises at least one of a swappable random access memory (RAM) and a swappable flash memory containing the predetermined security configuration.

26. (original) The security processor of claim 20 wherein the system for multi-stream security processing and distributing digital media streams comprises a headend, a network electrically coupled to the headend, a set top box (STB) coupled to the network, and a receiver coupled to the STB, and the security processor is implemented in connection with at least one of the headend, the network, the STB, and the receiver.

27. (original) The security processor of claim 20 wherein the security processor provides role-based authentication that is used by an authorized user for at least one of configuration, reconfiguration, and renewal.

28. (original) The security processor of claim 20 wherein the security processor is implemented in connection with a receiver or a transceiver that is at least one of a set top box (STB), and a receiver or transceiver for at least one of digital televison, high definition digital television (HDTV), audio, MP3, text messaging, and game digital streams.